

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2001-265687

(43)Date of publication of application : 28.09.2001

(51)Int.Cl.

G06F 13/00
 B41J 5/30
 B41J 29/38
 G03G 21/02
 G03G 21/00
 G06F 3/12
 G06F 15/00
 G06F 17/60

(21)Application number : 2000-076018 (71)Applicant : CANON INC

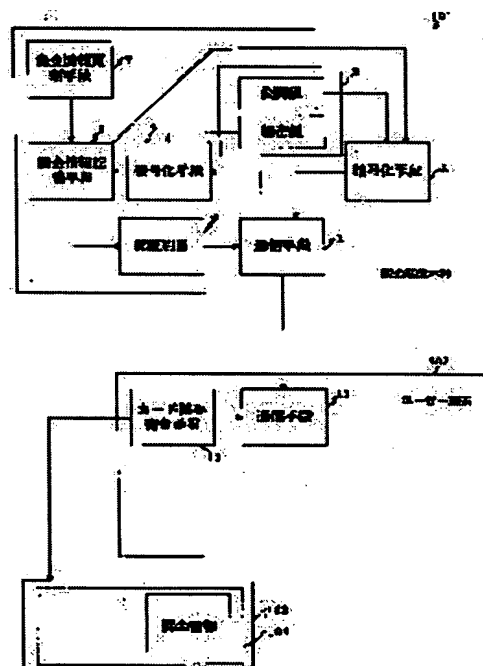
(22)Date of filing : 17.03.2000 (72)Inventor : SAIDA TADAAKI

(54) NETWORK SYSTEM, DEVICE AND METHOD FOR ACCOUNTING PROCESSING
 AND COMPUTER READABLE STORAGE MEDIUM

(57)Abstract:

PROBLEM TO BE SOLVED: To prevent the leakage of information without obstructing the effective utilization of a network environment and to perform charging processings for respective users on a network.

SOLUTION: This accounting processor 101 is provide with a key storage means 2 for storing a public key and a secret key, a communication means 1 for transmitting/receiving accounting information ciphered by using the public key, a deciphering means 4 for deciphering the ciphered accounting information by using the secret key, an authentication judgment means 6 for judging the propriety of use for a prescribed object on the basis of the deciphered charging information, an accounting information updating means 7 for updating the charging information by using conditions for the prescribed object and a ciphering means 3 for ciphering the updated accounting information by using the public key. Also, a user terminal 102 is provided with the communication means 11 for transmitting/receiving the accounting information ciphered by using the public key.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号
特開2001-265687
(P2001-265687A)

(43) 公開日 平成13年9月28日 (2001.9.28)

(51) Int.Cl. ⁷	識別記号	F I	テーマコード(参考)
G 0 6 F 13/00	3 5 4	G 0 6 F 13/00	3 5 4 Z 2 C 0 6 1
B 4 1 J 5/30		B 4 1 J 5/30	Z 2 C 0 8 7
29/38		29/38	Z 2 H 0 2 7
G 0 3 G 21/02		G 0 3 G 21/00	3 9 6 5 B 0 2 1
21/00	3 9 6	G 0 6 F 3/12	A 5 B 0 4 9

審査請求 未請求 請求項の数16 O L (全 11 頁) 最終頁に続く

(21) 出願番号 特願2000-76018(P2000-76018)

(22) 出願日 平成12年3月17日 (2000.3.17)

(71) 出願人 000001007

キヤノン株式会社

東京都大田区下丸子3丁目30番2号

(72) 発明者 斉田 忠明

東京都大田区下丸子3丁目30番2号 キヤ
ノン株式会社内

(74) 代理人 100090273

弁理士 國分 孝悦

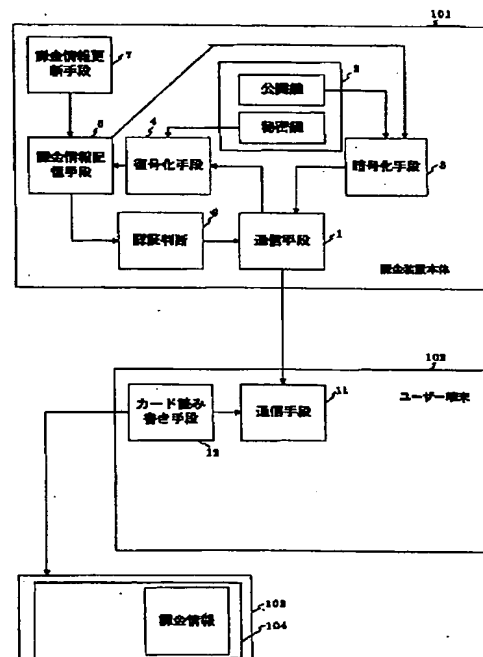
最終頁に続く

(54) 【発明の名称】 ネットワークシステム、課金処理装置、方法、及びコンピュータ読み取り可能な記憶媒体

(57) 【要約】

【課題】 ネットワーク環境の効率的な利用を妨げることなく、情報の漏洩を防止するとともに、ネットワーク上での各ユーザごとの課金処理を行う。

【解決手段】 課金処理装置101は、公開鍵及び秘密鍵を記憶する鍵記憶手段2と、公開鍵を用いて暗号化された課金情報を送受信する通信手段1と、暗号化された課金情報を秘密鍵を用いて復号化する復号化手段4と、復号化された課金情報に基づいて所定対象についての使用の可否を判断する認証判断手段6と、所定対象についての使用状況により課金情報を更新する課金情報更新手段7と、更新された課金情報を公開鍵を用いて暗号化する暗号化手段3とを具備し、又、ユーザ端末102は、公開鍵を用いて暗号化された課金情報を送受信する通信手段11を具備する。



の使用に対する課金処理を行う処理を実行するプログラムを格納したコンピュータ読み取り可能な記憶媒体であって、
 一対の公開鍵及び秘密鍵を記憶する処理と、
 上記公開鍵を用いて暗号化された課金情報を取得する処理と、
 上記暗号化された課金情報を上記秘密鍵を用いて復号化する処理と、
 上記復号化された課金情報に基づいて上記所定対象についての使用の可否を判断する処理と、
 上記所定対象についての使用状況により上記課金情報を更新する処理と、
 上記更新された課金情報を上記公開鍵を用いて暗号化する処理と、
 上記暗号化された上記更新後の課金情報を送出する処理とを実行するためのプログラムを格納することを特徴とするコンピュータ読み取り可能な記憶媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、ネットワークシステム、課金処理装置、方法、及びコンピュータ読み取り可能な記憶媒体に関し、特に、オフィス等のネットワーク環境における複写機等の使用に対して課金処理を行うのに用いて好適なものである。

【0002】

【従来の技術】従来の課金方式として、例えば複写機でのコピーに対する課金等は、機器が持つ動作カウンタにより行っていた。そして、定期的にサービスマンがレンタル先を訪問し、上記動作カウンタのカウント数に応じて徴収すべき金額を計算していた。

【0003】しかし、ハードウェアのカウントによる課金では、1台の機器に対するユーザごとの管理を行うことができない。又、サービスマンが機器の設置先を訪問する必要があり、効率が悪くなってしまう。

【0004】最近では、ソフトウェアを利用した課金も行われている。この場合、本体の動作カウンタをソフトウェア化し、その動作カウント数をメモリに記憶しておく。そして、その動作カウント数を、通信用ソフトウェアにより、電話回線等を介して課金を管理している管理センタに転送する。管理センタでは、転送されてきた動作カウント数に応じて金額を計算し、顧客に対して料金の請求を行う。これにより、遠隔地からの課金管理を行うことが可能となる。

【0005】しかし、ソフトウェアのカウントによる課金では、メモリ上に数値が書き込まれているだけであり、故意に上書きされる危険性がある。又、情報の漏洩というおそれもある。

【0006】又、ユーザそれぞれにユーザカードを持たせ、このユーザカードを利用して個人ごとの課金管理を行うこともなされている。ユーザカードには、一定の使

用限度が設定された課金情報が書き込まれている。ユーザは、機器を使用するときに、当該機器に設置されたカードリーダーに自分のユーザカードを挿入する。機器側では、ユーザカードから読み出された課金情報に基づき、使用限度を超えていない場合には機器の利用を許可し、その使用量に応じてユーザカードの課金情報を書き換える。一方、使用限度を超えている場合は、機器の使用を許可しない。

【0007】

10 【発明が解決しようとする課題】しかし、例えば、オフィス等のネットワーク環境において、プリンタ、スキャナ、複写等に対する課金処理を行うような場合に、ユーザカードを用いた課金管理を行うと、ネットワーク環境の効率的な利用が妨げられてしまうことがある。例えば、複写機本体をプリンタとして利用する場合に、複写機本体にユーザカードを挿入する方式では、ユーザは、まず複写機本体のある所まで行きユーザカードを差し込んでから、再びユーザ端末のある所に戻ってプリントデータを送信しなければならない。そういった動作をプリントしようとする度に行う必要があり、ネットワーク環境を効率的に利用することができなくなってしまう。

【0008】本発明は、上記のような課題を解決するためになされたものであり、ネットワーク環境の効率的な利用を妨げることなく、情報の漏洩を防止しつつ、ネットワーク上での各ユーザごとの課金処理を行うことを可能にすることを目的とする。

【0009】

30 【課題を解決するための手段】本発明のネットワークシステムは、第1の公開鍵及び第1の秘密鍵を記憶する鍵記憶手段、上記第1の公開鍵を用いて暗号化された課金情報を送受信する通信手段、上記暗号化された課金情報を上記第1の秘密鍵を用いて復号化する復号化手段、上記復号化された課金情報に基づいて所定対象についての使用の可否を判断する認証判断手段、上記所定対象についての使用状況により上記課金情報を更新する課金情報更新手段、上記更新された課金情報を上記第1の公開鍵を用いて暗号化する暗号化手段を具備する課金処理装置と、上記第1の公開鍵を用いて暗号化された課金情報を送受信する通信手段を具備するユーザ端末とを備えた点に特徴を有する。

【0010】本発明のネットワークシステムの他の特徴とするところは、上記ユーザ端末は、ユーザカードに対して、上記第1の公開鍵を用いて暗号化された課金情報の読み出し処理、書き込み処理を行うカード読み書き手段を有する点にある。

【0011】本発明のネットワークシステムの他の特徴とするところは、上記課金処理装置は、上記ユーザ端末に上記第1の公開鍵を送信する送信手段を有し、上記ユーザ端末は、上記所定対象についての使用に関するデータを上記第1の公開鍵を用いて暗号化する暗号化手段

102から送信される課金情報を記憶する。6は認証判断手段であり、上記課金情報に基づいて、図示しない機器のユーザによる使用の可否を判断する。7は課金情報更新手段であり、ユーザの使用状況により上記課金情報を更新する。

【0029】ユーザ端末102において、11は通信手段であり、上記複写機本体105との通信を行う。12はカード読み書き手段であり、カードリーダ103に挿入されたユーザカード104の読み書きを行う。

【0030】103はカードリーダである。104は各ユーザが所有するユーザカードであり、当該ユーザカード104には、ユーザの課金情報が書き込まれている。

【0031】次に、図1、2に基づいて上記ネットワークシステムの動作について説明する。ユーザは、ネットワークを介して図示しない機器を使用するときは、カードリーダ103に自己のユーザカード104を挿入するとともに、課金処理装置101に機器の使用要求を行う(2.1)。このとき、ユーザ端末102は、カード読み書き手段12によりユーザカード104から課金情報の読み出しを行う(2.2)。そして、この課金情報を、通信手段11を介して課金処理装置101に送信する(2.3)。なお、この課金情報は、詳しくは後述するが、上記公開鍵を用いて暗号化された状態となっている。

【0032】課金処理装置101では、通信部1を介して上記課金情報を受信したら、復号化手段4において、当該課金情報を鍵記憶手段2内の秘密鍵を用いて復号化する(2.4)。復号化手段4により復号化された課金情報は、課金情報記憶手段5に記憶される。

【0033】さらに、認証判断手段6において、上記課金情報に基づいてユーザの機器利用が可能かどうかを判断する(2.5)。そして、利用可能であれば、通信部1を介してユーザ端末102に認証通知を行う(2.6)。

【0034】上記のように認証通知を受け取ったならば、ユーザ端末102と課金処理装置101が管理する機器との間で動作のやり取りが行われる(2.7)。例えば、上記機器がプリンタであれば、ユーザ端末102からプリントデータが送信され、プリント処理が実行される。又、上記機器がスキャナであれば、スキャン処理が実行され、その結果得られたスキャンデータがユーザ端末102に送信される。

【0035】以上の動作が終了すると、課金処理装置101の課金情報更新手段7は、ユーザの機器の使用に応じて課金情報記憶手段5に記憶されている課金情報を更新する(2.8)。そして、その更新された課金情報を暗号化手段3において鍵記憶手段2内の公開鍵を用いて暗号化した上で(2.9)、通信手段1を介してユーザ端末102に送信する(2.10)。

【0036】ユーザ端末102では、更新された課金情報を受け取ったら、その課金情報をカード読み書き手段12を介してユーザカード104に書き込む(2.11)。

したがって、上述したように、更新された課金情報は、上記公開鍵を用いて暗号化された状態でユーザカード104に書き込まれた状態となる。

【0037】以上述べた第1の実施の形態によれば、課金情報を通信を介して送受信するようにしたので、各ユーザ端末102においてユーザカード104を利用することができる。これにより、例えば、ユーザがいちいち複写機のある所まで行きユーザカードを差し込んでから、再びユーザ端末のある所に戻ってプリントデータを送信するような手間が不要となる。

【0038】しかも、上記課金情報を公開鍵を用いて暗号化しているため、ネットワーク上での課金情報の漏洩を防止して、情報内容の機密性を保つことができる。

【0039】(第2の実施の形態)図3には、第2の実施の形態のネットワークシステムを示す。このネットワークシステムは、プリント機能及びスキャン機能を有する複写機本体105と、カードリーダ103が接続されたユーザ端末102とを備える。そして、この複写機本体105に課金処理装置を内蔵させている。

【0040】さらに、本実施の形態のネットワークシステムでは、詳しくは後述するが、課金情報だけでなく、複写機本体105の利用に関するデータについても暗号化、復号化を行うことにしている。以下、本実施の形態のネットワークシステムについて説明するが、上記第1の実施の形態で述べた構成要素と同一の要素には同一の符号を付し、その詳細な説明は省略する。

【0041】複写機本体105において、8はユーザ公開鍵記憶手段であり、ユーザ端末102から送信される後述するユーザ公開鍵を記憶する。9はプリント処理を実行するプリント手段である。10はスキャン処理を実行するスキャン手段である。

【0042】なお、通信手段1～課金情報更新手段7については、上記第1の実施の形態で説明した通りである。ただし、暗号化手段3は、上記鍵記憶手段2に記憶された公開鍵(以下、鍵記憶手段2に記憶された公開鍵を「複写機公開鍵」、秘密鍵を「複写機秘密鍵」と称する)を用いた暗号化だけでなく、上記ユーザ公開鍵記憶手段8に記憶されたユーザ公開鍵を用いた暗号化も行う。

【0043】ユーザ端末102において、13は復号化手段であり、ユーザ秘密鍵を用いた復号化を行う。14は複写機公開鍵記憶手段であり、複写機本体105から送信される複写機公開鍵を記憶する。15は暗号化手段であり、上記複写機公開鍵を用いた暗号化を行う。なお、通信手段11、カード読み書き手段12については、上記第1の実施の形態で説明した通りである。

【0044】103はカードリーダである。104は各ユーザが所有するユーザカードであり、当該ユーザカード104には、ユーザの課金情報に加えて、各ユーザごとに割り当てられたユーザ独自のユーザ公開鍵及びユー

対し、上記実施の形態の機能を実現するためのソフトウェアのプログラムコードを供給し、そのシステム或いは装置のコンピュータ（CPU或いはMPU）に格納されたプログラムに従って上記各種デバイスを動作させることによって実施したものも、本発明の範疇に含まれる。

【0062】又、この場合、上記ソフトウェアのプログラムコード自体が上述した実施の形態の機能を実現することになり、そのプログラムコード自体、及びそのプログラムコードをコンピュータに供給するための手段、例えばかかるプログラムコードを格納した記録媒体は本発明を構成する。かかるプログラムコードを記憶する記録媒体としては、例えばフロッピー（登録商標）ディスク、ハードディスク、光ディスク、光磁気ディスク、CD-ROM、磁気テープ、不揮発性のメモ리카ード、ROM等を用いることができる。

【0063】又、コンピュータが供給されたプログラムコードを実行することにより、上述の実施の形態の機能が実現されるだけでなく、そのプログラムコードがコンピュータにおいて稼働しているOS（オペレーティングシステム）或いは他のアプリケーションソフト等と共同して上述の実施の形態の機能が実現される場合にもかかるプログラムコードは本発明の実施の形態に含まれることはいうまでもない。

【0064】さらに、供給されたプログラムコードがコンピュータの機能拡張ボードやコンピュータに接続された機能拡張ユニットに備わるメモリに格納された後、そのプログラムコードの指示に基づいてその機能拡張ボードや機能拡張ユニットに備わるCPU等が実際の処理の一部又は全部を行い、その処理によって上述した実施の形態の機能が実現される場合にも本発明に含まれることはいうまでもない。

【0065】なお、上記実施の形態において示した各部の形状及び構造は、何れも本発明を実施するにあたっての具体化のほんの一例を示したものに過ぎず、これらによって本発明の技術的範囲が限定的に解釈されてはならないものである。すなわち、本発明はその精神、又はその主要な特徴から逸脱することなく、様々な形で実施することができる。

【0066】

【発明の効果】以上述べたように本発明によれば、ネットワーク環境の効率的な利用を妨げることなく、ネットワーク上での各ユーザごとの課金処理を行うことができる。しかも、課金情報を暗号化するので、ネットワーク上の課金情報の機密性を保つことができる。

【図面の簡単な説明】

【図1】第1の実施の形態のネットワークシステムの構成を示す図である。

【図2】第1の実施の形態のネットワークシステムでの各手段の動作について説明するための図である。

【図3】第2の実施の形態のネットワークシステムの構成を示す図である。

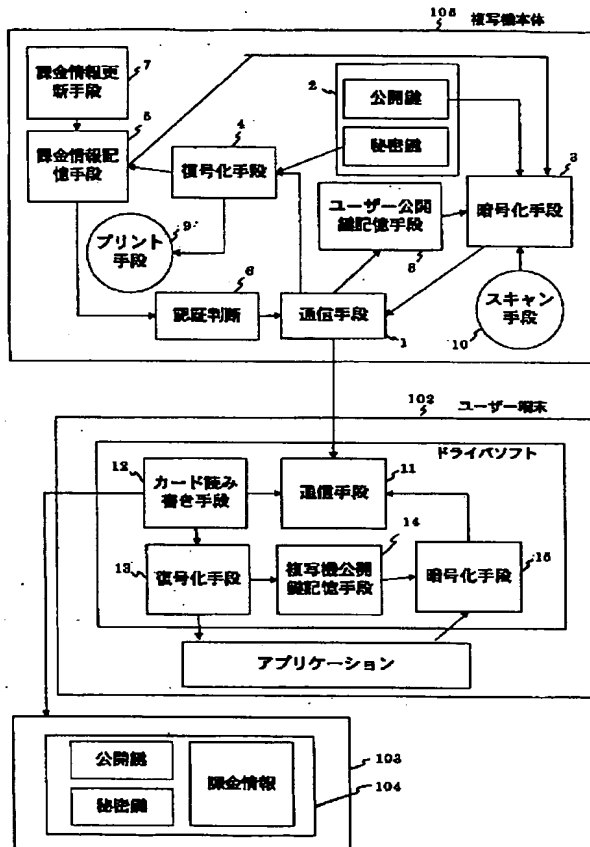
【図4】第2の実施の形態のネットワークシステムでプリント要求を行った場合の各手段の動作について説明するための図である。

【図5】第2の実施の形態のネットワークシステムでスキャン要求を行った場合の各手段の動作について説明するための図である。

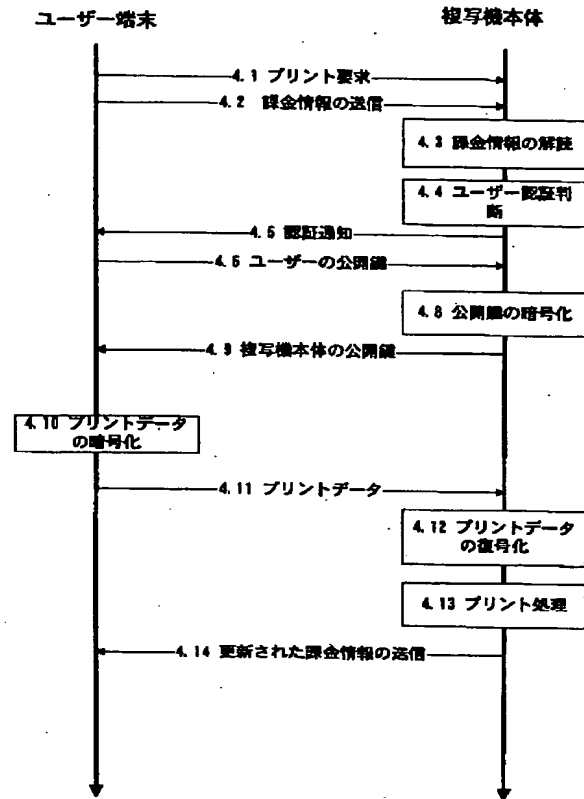
【符号の説明】

101	課金処理装置
102	ユーザ端末
103	カードリーダー
104	ユーザカード
105	複写機本体
1	通信手段
2	鍵記憶手段
3	暗号化手段
4	復号化手段
5	課金情報記憶手段
6	認証判断手段
7	課金情報更新手段
8	ユーザ公開鍵記憶手段
9	プリント手段
10	スキャン手段
11	通信手段
12	カード読み書き手段
13	復号化手段
14	複写機公開鍵記憶手段
15	暗号化手段

【図3】



【図4】



F ターム(参考) 2C061 AP01 AP04 HH01 HJ06 HJ10
HK04 HK11 HN05 HN11 HN15
2C087 AB06 BA14 BC12 BD24 BD53
CB02 CB03
2H027 EE10 EJ02 EJ03 EJ05 EJ06
EJ08 EJ15 ZA07
5B021 AA01 AA21 BB04 CC05 CC07
5B049 AA05 CC36 DD00 DD04 EE01
EE23 EE28 FF02 FF08 GG04
GG07 GG09 GG10
5B085 AA08 AE29
5B089 GA11 GA21 JB22 KA15 KA17
KB12 KB13 KC58 KH30 LB06
LB12 LB26
9A001 BB04 CC08 EE03 JJ12 JJ35
JJ64 KK42 LL03 LL09

*** NOTICES ***

Japan Patent Office is not responsible for any damages caused by the use of this translation.

1. This document has been translated by computer. So the translation may not reflect the original precisely.
2. **** shows the word which can not be translated.
3. In the drawings, any words are not translated.

CLAIMS

[Claim(s)]

[Claim 1] A key storage means to memorize the 1st public key and 1st private key, the means of communications which transmit and receive the accounting information enciphered using the 1st public key of the above, A decryption means to decrypt the accounting information by which encryption was carried out [above-mentioned] using the 1st private key of the above, An authentication decision means to judge the propriety of the activity about a predetermined object based on the accounting information by which the decryption was carried out [above-mentioned], The accounting equipment possessing a renewal means of accounting information to update the above-mentioned accounting information according to the operating condition about the above-mentioned predetermined object, and an encryption means to encipher the accounting information by which updating was carried out [above-mentioned] using the 1st public key of the above, The network system characterized by having a user terminal possessing the means of communications which transmits and receives the accounting information enciphered using the 1st public key of the above.

[Claim 2] The above-mentioned user terminal is a network system according to claim 1 characterized by having a card R/W means to perform read-out processing of the accounting information enciphered using the 1st public key of the above, and write-in processing, to a user card.

[Claim 3] The above-mentioned accounting equipment is a network system according to claim 1 or 2 carried out [that have a transmitting means transmit the 1st public key of the above to the above-mentioned user terminal, and the above-mentioned user terminal has an encryption means to encipher the data about the activity about the above-mentioned predetermined object using the 1st public key of the above, and a transmitting means transmit the data by which encryption was carried out / above-mentioned / to the above-mentioned accounting equipment, and] as the description.

[Claim 4] The above-mentioned accounting equipment is a network system according to claim 3 characterized by having a decryption means to decrypt the data which were received from the above-mentioned user terminal, and by which encryption was carried out [above-mentioned] using the 1st private key of the above.

[Claim 5] The network system according to claim 3 or 4 characterized by for the activity about the above-mentioned predetermined object being an activity of a print function, and the data about the activity about the above-mentioned predetermined object being print

data.

[Claim 6] The above-mentioned user terminal is a network system according to claim 1 or 2 characterized by having an encryption means to encipher data to have a transmitting means to transmit a user's 2nd original public key, and concerning [the above-mentioned accounting equipment] the activity about the above-mentioned predetermined object using the 2nd public key of the above, and a transmitting means to transmit the data by which encryption was carried out [above-mentioned] to the above-mentioned user terminal.

[Claim 7] The above-mentioned user terminal is a network system according to claim 6 characterized by having a decryption means to decrypt the data which were received from the above-mentioned accounting equipment, and by which encryption was carried out [above-mentioned] using the 2nd private key corresponding to the 2nd public key of the above.

[Claim 8] The network system according to claim 6 or 7 characterized by for the activity about the above-mentioned predetermined object being an activity of a scanning function, and the data about the activity about the above-mentioned predetermined object being scanning data.

[Claim 9] A key storage means to perform accounting to the activity about a predetermined object based on accounting information and to be accounting equipment and to memorize the public key and private key of a couple, An accounting information acquisition means to acquire the above-mentioned accounting information enciphered using the above-mentioned public key, A decryption means to decrypt the accounting information by which encryption was carried out [above-mentioned] using the above-mentioned private key, An authentication decision means to judge the propriety of the activity about the above-mentioned predetermined object based on the accounting information by which the decryption was carried out [above-mentioned], A renewal means of accounting information to update the above-mentioned accounting information according to the operating condition about the above-mentioned predetermined object, Accounting equipment characterized by having an encryption means to encipher the accounting information by which updating was carried out [above-mentioned] using the above-mentioned public key, and an accounting information sending-out means to send out the accounting information after the renewal of the above by which encryption was carried out [above-mentioned].

[Claim 10] Accounting equipment according to claim 9 characterized by having the means of communications for performing the communication link with the exterior, and constituting the above-mentioned accounting information acquisition means and the above-mentioned accounting information sending-out means by the means of communications concerned.

[Claim 11] Accounting equipment according to claim 10 characterized by making the above-mentioned public key into ready-for-sending ability through the above-mentioned means of communications.

[Claim 12] Accounting equipment according to claim 11 characterized by making into ability ready for receiving the predetermined data enciphered using the above-mentioned public key through the above-mentioned means of communications.

[Claim 13] Accounting equipment according to claim 10 characterized by making a public

key other than the above-mentioned public key into ability ready for receiving through the above-mentioned means of communications.

[Claim 14] Accounting equipment according to claim 13 characterized by making into ready-for-sending ability the data which were equipped with an encryption means to encipher using the public key according to above of predetermined data, and were enciphered through the above-mentioned means of communications using the public key according to above.

[Claim 15] The procedure of being the accounting approach of performing accounting to the activity about a predetermined object based on accounting information, and memorizing the public key and private key of a couple, The procedure which acquires the accounting information enciphered using the above-mentioned public key, and the procedure which decrypts the accounting information by which encryption was carried out

[above-mentioned] using the above-mentioned private key, The procedure of judging the propriety of the activity about the above-mentioned predetermined object based on the accounting information by which the decryption was carried out [above-mentioned], The accounting approach characterized by having the procedure which updates the above-mentioned accounting information according to the operating condition about the above-mentioned predetermined object, the procedure which enciphers the accounting information by which updating was carried out [above-mentioned] using the above-mentioned public key, and the procedure which sends out the accounting information after the renewal of the above by which encryption was carried out [above-mentioned].

[Claim 16] The processing which is the storage which stored the program which performs processing which performs accounting to the activity about a predetermined object based on accounting information, and in which computer reading is possible, and memorizes the public key and private key of a couple, The processing which acquires the accounting information enciphered using the above-mentioned public key, and the processing which decrypts the accounting information by which encryption was carried out

[above-mentioned] using the above-mentioned private key, The processing which judges the propriety of the activity about the above-mentioned predetermined object based on the accounting information by which the decryption was carried out [above-mentioned], The processing which updates the above-mentioned accounting information according to the operating condition about the above-mentioned predetermined object, The storage which is characterized by storing the program for performing processing which enciphers the accounting information by which updating was carried out [above-mentioned] using the above-mentioned public key, and processing which sends out the accounting information after the renewal of the above by which encryption was carried out [above-mentioned] and in which computer reading is possible.

DETAILED DESCRIPTION

[Detailed Description of the Invention]

[0001]

[Field of the Invention] This invention is used for performing accounting to the activity of the copying machine in an office etc. network environment etc. especially about a network system, accounting equipment, an approach, and the storage in which computer reading is possible, and is suitable.

[0002]

[Description of the Prior Art] As a conventional charging system, the counter of operation which a device has was performing accounting to the copy in a copying machine etc. And periodically, the serviceman visited the rental place and the amount of money which should be collected according to the number of counts of the above-mentioned counter of operation was calculated.

[0003] However, in accounting by the count of hardware, not every user to one set of a device is manageable. Moreover, a serviceman will need to visit the installation place of a device and effectiveness will worsen.

[0004] Recently, accounting using software is also performed. In this case, the counter of a body of operation is software-ized and that number of counts of operation is memorized in memory. And the number of counts of operation is transmitted to the management center which has managed accounting through the telephone line etc. with the software for a communication link. In the management center, the amount of money is calculated according to the transmitted number of counts of operation, and a customer is asked for a tariff. This becomes possible to perform accounting management from a remote place.

[0005] However, in accounting by the count of software, the numeric value is only written in on memory and there is a danger of being overwritten intentionally. Moreover, there is also a possibility of calling it informational leakage.

[0006] Moreover, a user card is given to each user and performing accounting management for every individual using this user card is also made. The accounting information to which the fixed operating limit was set is written in the user card. A user inserts his own user card in the card reader installed in the device concerned, when using a device. In a device side, when it is not over the operating limit based on the accounting information by which reading appearance was carried out from a user card, utilization of a device is permitted, and the accounting information of a user card is rewritten according to the amount used. On the other hand, the activity of a device is not permitted when it is over the operating limit.

[0007]

[Problem(s) to be Solved by the Invention] However, if accounting management which used the user card is performed in an office etc. network environment for example, when performing accounting to a printer, a scanner, a copy, etc., efficient utilization of a network environment may be barred. For example, by the method which inserts a user card in the body of a copying machine, when using the body of a copying machine as a printer, after going to the place which has a body of a copying machine first and inserting a user card, a user has to return to the place which has a user terminal again, and has to transmit print data. It will become impossible to carry out, whenever it is going to print such actuation, and to use a network environment efficiently.

[0008] This invention aims at making it possible to perform accounting for every user on a network, preventing informational leakage without being made in order to solve the above

technical problems, and barring efficient utilization of a network environment.

[0009]

[Means for Solving the Problem] A key storage means by which the network system of this invention memorizes the 1st public key and 1st private key, The means of communications which transmits and receives the accounting information enciphered using the 1st public key of the above, A decryption means to decrypt the accounting information by which encryption was carried out [above-mentioned] using the 1st private key of the above, An authentication decision means to judge the propriety of the activity about a predetermined object based on the accounting information by which the decryption was carried out [above-mentioned], The accounting equipment possessing a renewal means of accounting information to update the above-mentioned accounting information according to the operating condition about the above-mentioned predetermined object, and an encryption means to encipher the accounting information by which updating was carried out [above-mentioned] using the 1st public key of the above, It has the description at the point equipped with the user terminal possessing the means of communications which transmits and receives the accounting information enciphered using the 1st public key of the above.

[0010] The place by which it is characterized [of the network system of this invention / other] has the above-mentioned user terminal in the point of having a card R/W means to perform read-out processing of the accounting information enciphered using the 1st public key of the above, and write-in processing, to a user card.

[0011] The place by which it is characterized [of the network system of this invention / other] has a transmitting means transmit the 1st public key of the above to the above-mentioned user terminal, and the above-mentioned accounting equipment is [place] in the above-mentioned user terminal to the point which it has about an encryption means encipher the data about the activity about the above-mentioned predetermined object using the 1st public key of the above, and a transmitting means transmit the data by which encryption was carried out [above-mentioned] to the above-mentioned accounting equipment.

[0012] The place by which it is characterized [of the network system of this invention / other] has the above-mentioned accounting equipment in the point of having a decryption means to decrypt the data which were received from the above-mentioned user terminal and by which encryption was carried out [above-mentioned] using the 1st private key of the above.

[0013] The activity about the above-mentioned predetermined object is an activity of a print function, and the data about the activity about the above-mentioned predetermined object have the place by which it is characterized [of the network system of this invention / other] in the point which is print data.

[0014] The above-mentioned user terminal has a transmitting means transmit a user's 2nd original public key, and the place by which it is characterized [of the network system of this invention / other] has the above-mentioned accounting equipment in the point of having an encryption means to encipher the data about the activity about the above-mentioned predetermined object using the 2nd public key of the above, and a transmitting means to transmit the data by which encryption was carried out [above-mentioned] to the above-mentioned user terminal.

[0015] The place by which it is characterized [of the network system of this invention / other] has the above-mentioned user terminal in the point of having a decryption means to decrypt the data which were received from the above-mentioned accounting equipment and by which encryption was carried out [above-mentioned] using the 2nd private key corresponding to the 2nd public key of the above.

[0016] The activity about the above-mentioned predetermined object is an activity of a scanning function, and the data about the activity about the above-mentioned predetermined object have the place by which it is characterized [of the network system of this invention / other] in the point which is scanning data.

[0017] Moreover, a key storage means for the accounting equipment of this invention to be accounting equipment which performs accounting to the activity about a predetermined object based on accounting information, and to memorize the public key and private key of a couple, An accounting information acquisition means to acquire the above-mentioned accounting information enciphered using the above-mentioned public key, A decryption means to decrypt the accounting information by which encryption was carried out [above-mentioned] using the above-mentioned private key, An authentication decision means to judge the propriety of the activity about the above-mentioned predetermined object based on the accounting information by which the decryption was carried out [above-mentioned], It has the description at the point equipped with a renewal means of accounting information to update the above-mentioned accounting information according to the operating condition about the above-mentioned predetermined object, an encryption means to encipher the accounting information by which updating was carried out [above-mentioned] using the above-mentioned public key, and an accounting information sending-out means to send out the accounting information after the renewal of the above by which encryption was carried out [above-mentioned].

[0018] The place by which it is characterized [of the accounting equipment of this invention / other] is equipped with the means of communications for performing the communication link with the exterior, and is in the point which constitutes the above-mentioned accounting information acquisition means and the above-mentioned accounting information sending-out means by the means of communications concerned.

[0019] The place by which it is characterized [of the accounting equipment of this invention / other] is in the point which made the above-mentioned public key ready-for-sending ability through the above-mentioned means of communications.

[0020] The place by which it is characterized [of the accounting equipment of this invention / other] is in the point which made the predetermined data enciphered using the above-mentioned public key ability ready for receiving through the above-mentioned means of communications.

[0021] The place by which it is characterized [of the accounting equipment of this invention / other] is in the point which made the public key other than the above-mentioned public key ability ready for receiving through the above-mentioned means of communications.

[0022] The place by which it is characterized [of the accounting equipment of this invention / other] is equipped with an encryption means to encipher using the public key according to above of predetermined data, and is in the point which made the data

enciphered using the public key according to above ready-for-sending ability through the above-mentioned means of communications.

[0023] Moreover, the procedure of the accounting approach of this invention being the accounting approach of performing accounting to the activity about a predetermined object based on accounting information, and memorizing the public key and private key of a couple, The procedure which acquires the accounting information enciphered using the above-mentioned public key, and the procedure which decrypts the accounting information by which encryption was carried out [above-mentioned] using the above-mentioned private key, The procedure of judging the propriety of the activity about the above-mentioned predetermined object based on the accounting information by which the decryption was carried out [above-mentioned], It has the description at the point of having the procedure which updates the above-mentioned accounting information according to the operating condition about the above-mentioned predetermined object, the procedure which enciphers the accounting information by which updating was carried out [above-mentioned] using the above-mentioned public key, and the procedure which sends out the accounting information after the renewal of the above by which encryption was carried out [above-mentioned].

[0024] Moreover, the storage which can computer read this invention The processing which is the storage which stored the program which performs processing which performs accounting to the activity about a predetermined object based on accounting information, and in which computer reading is possible, and memorizes the public key and private key of a couple, The processing which acquires the accounting information enciphered using the above-mentioned public key, and the processing which decrypts the accounting information by which encryption was carried out [above-mentioned] using the above-mentioned private key, The processing which judges the propriety of the activity about the above-mentioned predetermined object based on the accounting information by which the decryption was carried out [above-mentioned], It has the description to the point stored in the program for performing processing which updates the above-mentioned accounting information according to the operating condition about the above-mentioned predetermined object, processing which enciphers the accounting information by which updating was carried out [above-mentioned] using the above-mentioned public key, and processing which sends out the accounting information after the renewal of the above by which encryption was carried out [above-mentioned].

[0025]

[Embodiment of the Invention] Hereafter, the network system of the gestalt of operation of this invention, accounting equipment, an approach, and the storage in which computer reading is possible are explained with reference to a drawing.

[0026] (Gestalt of the 1st operation) The network system of the gestalt of the 1st operation is shown in drawing 1 . This network system is equipped with the user terminal 102 by which the card reader 103 was connected with the accounting equipment 101 which performs accounting about the activity of the device which is not illustrated.

[0027] In accounting equipment 101, 1 is means of communications and performs the communication link with a user terminal 102. 2 is a key storage means and memorizes the public key and private key of a couple. 3 is an encryption means and performs encryption

using the above-mentioned public key. 4 is a decryption means and performs the decryption using the above-mentioned private key.

[0028] 5 is an accounting information storage means and memorizes the accounting information transmitted from a user terminal 102. 6 is an authentication decision means and judges the propriety of the activity by the user of a device who does not illustrate based on the above-mentioned accounting information. 7 is a renewal means of accounting information, and updates the above-mentioned accounting information according to a user's operating condition.

[0029] In a user terminal 102, 11 is means of communications and performs the communication link with the above-mentioned body 105 of a copying machine. 12 is a card R/W means and write the user card 104 inserted in the card reader 103. [reading and]

[0030] 103 is a card reader. 104 is a user card which each user owns, and a user's accounting information is written in the user card 104 concerned.

[0031] Next, actuation of the above-mentioned network system is explained based on drawing 1 and 2. A user gives the activity demand of a device to accounting equipment 101 while inserting the user card 104 of self in a card reader 103, when using the device which is not illustrated through a network (2.1). At this time, a user terminal 102 reads accounting information from the user card 104 with the card R/W means 12 (2.2). And this accounting information is transmitted to accounting equipment 101 through means of communications 11 (2.3). In addition, although this accounting information is mentioned later in detail, it is in the condition of having been enciphered using the above-mentioned public key.

[0032] With accounting equipment 101, if the above-mentioned accounting information is received through the communications department 1, in the decryption means 4, the accounting information concerned will be decrypted using the private key within the key storage means 2 (2.4). The accounting information decrypted by the decryption means 4 is memorized by the accounting information storage means 5.

[0033] Furthermore, in the authentication decision means 6, it judges whether device utilization of a user is possible based on the above-mentioned accounting information (2.5). And if available, advice of authentication will be performed to a user terminal 102 through the communications department 1 (2.6).

[0034] If advice of authentication is received as mentioned above, an exchange of operation will be performed between a user terminal 102 and the device which accounting equipment 101 manages (2.7). For example, if the above-mentioned device is a printer, print data will be transmitted from a user terminal 102, and print processing will be performed. Moreover, if the above-mentioned device is a scanner, scanning and processing will be performed and the scanning data obtained as a result will be transmitted to a user terminal 102.

[0035] After the above actuation is completed, the renewal means 7 of accounting information of accounting equipment 101 updates the accounting information memorized by the accounting information storage means 5 according to the activity of a user's device (2.8). And after enciphering the updated accounting information using the public key within the key storage means 2 in the encryption means 3, it transmits to a user terminal 102 through (2.9) and means of communications 1 (2.10).

[0036] In a user terminal 102, if the updated accounting information is received, the

accounting information will be written in the user card 104 through the card R/W means 12 (2.11). Therefore, as mentioned above, the updated accounting information will be in the condition of having been written in the user card 104 in the condition of having been enciphered using the above-mentioned public key.

[0037] According to the gestalt of the 1st operation described above, since accounting information was transmitted and received through the communication link, the user card 104 can be used in each user terminal 102. After a user goes to the place which has a copying machine one by one and inserts a user card by this, time and effort which returns to the place which has a user terminal again, and transmits print data becomes unnecessary.

[0038] And since the above-mentioned accounting information is enciphered using a public key, leakage of the accounting information on a network can be prevented and the confidentiality of the content of information can be maintained.

[0039] (Gestalt of the 2nd operation) The network system of the gestalt of the 2nd operation is shown in drawing 3. This network system is equipped with the user terminal 102 by which the card reader 103 was connected with the body 105 of a copying machine which has a print function and a scanning function. And accounting equipment is made to build in this body 105 of a copying machine.

[0040] Furthermore, in the network system of the gestalt of this operation, although mentioned later in detail, encryption and a decryption are performed also about the data about utilization of not only accounting information but the body 105 of a copying machine. Hereafter, although the network system of the gestalt of this operation is explained, the same sign is given to the same element as the component stated with the gestalt of implementation of the above 1st, and the detailed explanation is omitted.

[0041] In the body 105 of a copying machine, 8 is a user public key storage means, and memorizes the user public key which is transmitted from a user terminal 102 and which is mentioned later. 9 is a print means to perform print processing. 10 is a scanning means to perform scanning and processing.

[0042] In addition, it is as the gestalt of implementation of the above 1st having explained means of communications 1 - the renewal means 7 of accounting information. However, the encryption means 3 performs not only the encryption using the public key (the public key memorized by the key storage means 2 is hereafter called a "copying machine public key", and a private key is called a "copying machine private key") memorized by the above-mentioned key storage means 2 but encryption using the user public key memorized by the above-mentioned user public key storage means 8.

[0043] In a user terminal 102, 13 is a decryption means and performs the decryption using a user private key. 14 is a copying machine public key storage means, and memorizes the copying machine public key transmitted from the body 105 of a copying machine. 15 is an encryption means and performs encryption using the above-mentioned copying machine public key. In addition, it is as the gestalt of implementation of the above 1st having explained means of communications 11 and the card R/W means 12.

[0044] 103 is a card reader. 104 is a user card which each user owns, and, in addition to a user's accounting information, a user's original user public key and user private key which were assigned for every user are written in the user card 104 concerned.

[0045] Next, actuation of the above-mentioned network system is explained based on drawing 3 -5. The actuation at the time of performing a print request to drawing 4 is shown, and the actuation at the time of giving a scanning demand to drawing 5 is shown.

[0046] A user inserts the user card 104 of self in a card reader 103, when performing a print request and a scanning demand. And a print request or a scanning demand is performed from the application of a user terminal 102 to the body 105 of a copying machine (4.1 of drawing 4 , 5.1 of drawing 5).

[0047] At this time, a user terminal 102 reads accounting information from the user card 104 with the card R/W means 12. As the gestalt of implementation of the above 1st also described, this accounting information is in the condition of having been enciphered using the copying machine public key. And this accounting information is transmitted to the body 105 of a copying machine through means of communications 11 (4.2 of drawing 4 , 5.2 of drawing 5).

[0048] By the body 105 of a copying machine, if the above-mentioned accounting information is received through the communications department 1, in the decryption means 4, the accounting information concerned will be decrypted using the copying machine private key within the key storage means 2. The accounting information decrypted by the decryption means 4 is memorized by the accounting information storage means 5 (4.3 of drawing 4 , 5.3 of drawing 5).

[0049] Furthermore, in the authentication decision means 6, it judges whether utilization of a user's body 105 of a copying machine is possible based on the above-mentioned accounting information (4.4 of drawing 2 , 5.4 of drawing 3). And if available, advice of authentication will be performed to a user terminal 102 through the communications department 1 (4.5 of drawing 2 , 5.6 of drawing 3).

[0050] the actuation so far -- a print request and a scanning demand -- in any case, it is the same, but since it differs by the case where a scanning demand is given to the case where a print request is carried out, subsequent actuation is explained, respectively.

[0051] First, explanation of the case where a print request is performed based on drawing 4 transmits a user public key from a user terminal 10 (4.6). The body 105 of a copying machine will encipher a copying machine public key using the user public key, if a user public key is received (4.8). And the body 105 of a copying machine transmits the enciphered copying machine public key to a user terminal 102 (4.9).

[0052] In a user terminal 102, the copying machine public key transmitted from the body 105 of a copying machine is memorized for the copying machine public key storage means 14. And delivery is used for print data from application, the above-mentioned copying machine public key is used for the encryption means 15 for the print data concerned, and it enciphers (4.10). This enciphered print data is transmitted to the body 105 of a copying machine through means of communications 11 (4.11).

[0053] By the body 105 of a copying machine, the print data which were transmitted from the user terminal 102 and by which encryption was carried out [above-mentioned] are sent to the decryption means 4. With the decryption means 4, the print data concerned are decrypted using the copying machine private key memorized by the key storage means 2 (4.12). And delivery and print processing are performed for the decrypted print data for the print means 9 (4.13).

[0054] Next, if the case where a scanning demand is performed based on drawing 5 is explained, the user terminal 102 which carried out the scanning demand will read the user public key in the user card 104 with the card R/W means 12, and will transmit the user public key to the body 105 of a copying machine (5.7).

[0055] By the body 105 of a copying machine, after memorizing the user public key transmitted from the user terminal 102 for the user public key storage means 8, scanning and processing are performed with the scanning means 10. And delivery is used for the image data (scanning data) obtained with the scanning means 10, the above-mentioned user public key is used for the encryption means 3 for the image data concerned, and it enciphers (5.8). This enciphered image data is transmitted to a user terminal 102 through means of communications 1 (5.9).

[0056] In a user terminal 102, the image data which was transmitted from the body 105 of a copying machine and by which encryption was carried out [above-mentioned] is sent to the decryption means 13. With the decryption means 13, a user private key is read from the user card 104, and the image data concerned is decrypted using the user private key (5.10). And the decrypted image data is sent to application, and processing of saving at a file is made.

[0057] After print actuation or scanning actuation is completed as mentioned above, the renewal means 7 of accounting information of the body 105 of a copying machine updates the accounting information memorized by the accounting information storage means 5 according to a user's activity. And the updated accounting information is transmitted to a user terminal 102 through means of communications 1, after enciphering using the copying machine public key within the key storage means 2 (4.14 of drawing 4 , 5.11 of drawing 5).

[0058] In a user terminal 102, if the updated accounting information is received, the accounting information will be written in the user card 104 through the card R/W means 12. Therefore, as mentioned above, the updated accounting information will be in the condition of having been written in the user card 104 in the condition of having been enciphered using the above-mentioned public key.

[0059] According to the gestalt of the 2nd operation, in addition to the effectiveness which was described above and which was stated with the gestalt of implementation of the above 1st, the data about the activity of the bodies 105 of a copying machine, such as print data and scanning data, can be enciphered, and the confidentiality of the data on a network can be raised more.

[0060] (Gestalt of other operations) Even if it applies this invention to the system which consists of two or more devices (for example, a host computer, an interface device, a reader, a printer, etc.), it may be applied to the equipment which consists of one device (for example, a copying machine, facsimile apparatus).

[0061] Moreover, so that various kinds of devices may be operated in order to realize the function of the gestalt of operation mentioned above As opposed to the computer in the equipment connected with these various devices, or a system The program code of the software for realizing the function of the gestalt of the above-mentioned implementation is supplied. What was carried out by operating the various above-mentioned devices according to the program stored in the computer (CPU or MPU) of the system or

equipment is contained under the category of this invention.

[0062] Moreover, the function of the gestalt of operation which the program code of the above-mentioned software itself mentioned above in this case will be realized, and the record medium which stored the means for supplying that program code itself and its program code to a computer, for example, this program code, constitutes this invention. As a record medium which memorizes this program code, a floppy (trademark) disk, a hard disk, an optical disk, a magneto-optic disk, CD-ROM, a magnetic tape, the memory card of a non-volatile, ROM, etc. can be used, for example.

[0063] Moreover, by performing the program code with which the computer was supplied, also when the function of the gestalt of above-mentioned operation is not only realized, but the function of the gestalt of above-mentioned operation is realized in collaboration with OS (operating system) or other application software etc. with which the program code is working in a computer, it cannot be overemphasized that this program code is contained in the gestalt of operation of this invention.

[0064] Furthermore, after stored in the memory with which the functional expansion unit by which the supplied program code was connected to the functional add-in board and the computer of a computer is equipped, also when the function of the gestalt of operation which the CPU with which the functional add-in board and functional expansion unit are equipped based on directions of the program code performed a part or all of actual processing, and mentioned above by the processing is realized, it cannot be overemphasized that it is contained in this invention.

[0065] In addition, it passes over no the configurations and structures of each part which were shown in the gestalt of the above-mentioned implementation to what showed a mere example of the somatization which hits carrying out this invention, and the technical range of this invention must not be restrictively interpreted by these. That is, this invention can be carried out in various forms, without deviating from the pneuma or its main description.

[0066]

[Effect of the Invention] Accounting for every user on a network can be performed without barring efficient utilization of a network environment according to this invention, as stated above. And since accounting information is enciphered, the confidentiality of the accounting information on a network can be maintained.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]

[Drawing 1] It is drawing showing the 1st configuration of the network system of the gestalt of operation.

[Drawing 2] It is drawing for explaining actuation of each means in the network system of the gestalt of the 1st operation.

[Drawing 3] It is drawing showing the 2nd configuration of the network system of the gestalt of operation.

[Drawing 4] It is drawing for explaining actuation of each means when the network system of the gestalt of the 2nd operation performs a print request.

[Drawing 5] It is drawing for explaining actuation of each means when the network system of the gestalt of the 2nd operation performs a scanning demand.

[Description of Notations]

101 Accounting Equipment

102 User Terminal

103 Card Reader

104 User Card

105 Body of Copying Machine

1 Means of Communications

2 Key Storage Means

3 Encryption Means

4 Decryption Means

5 Accounting Information Storage Means

6 Authentication Decision Means

7 Renewal Means of Accounting Information

8 User Public Key Storage Means

9 Print Means

10 Scanning Means

11 Means of Communications

12 Card R/W Means

13 Decryption Means

14 Copying Machine Public Key Storage Means

15 Encryption Means